Common Criteria

Evaluation and Validation Scheme

for

Information Technology Security

Validation Body Standard Operating Procedures

Scheme Publication #2

DRAFT

Version 1.5

May 2000

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Systems Security Organization
9800 Savage Road
Fort George G. Meade, MD 20755

This page intentionally left blank

1 Introduction

The Common Criteria Evaluation and Validation Scheme (CCEVS) for Information Technology Security was established by the National Information Assurance Partnership (NIAP), a partnership established by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) to evaluate conformance of Information Technology (IT) products and specifications (protection profiles) to international standards. Currently, the CCEVS scope covers information technology products and protection profiles evaluated against the *Common Criteria for Information Technology Security Evaluation* (CC) at Evaluation Assurance Levels (EAL) 1 through 4. The principal participants in the program are the Sponsors of IT product or protection profile evaluations, the product or protection profile developer, the Common Criteria Testing Laboratories (CCTLs) and the CCEVS Validation Body.

A Sponsor is the party requesting and paying for the security evaluation of an IT product or protection profile (PP) conducted by a CCTL. The Sponsor may be the developer of a protection profile, the developer of a product, a value-added reseller of a product, or another party that wishes to have a product evaluated.

A CCTL is a commercial testing laboratory accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to perform security evaluations against the *Common Criteria for Information Technology Security Evaluation* (CC) using the *Common Evaluation Methodology for Information Technology Security Evaluation* (CEM).

The CCEVS Validation Body, hereafter referred to as the Validation Body, is the government organization established by the NIAP to implement and operate the evaluation scheme for the U.S. government. This document, the second in a series of CCEVS publications, describes the standard operating procedures and quality program for the Validation Body.

[ISO65 4.1.3, CCMRA Article 4]

1.1 Background

The CC is a set of functional and assurance IT security requirements that was developed by the governments of the United States, Canada, France, Germany, the Netherlands, and the United Kingdom. The purpose of the CC is to provide a common international language in which to express IT security requirements. The CEM was also jointly developed by the same countries to establish a common approach for conducting IT security evaluations against the CC. The ultimate goal of these efforts is to have the results of an evaluation performed by one participating country recognized by another participating country without the product having to be evaluated and certified/validated again.

On October 5, 1998, the *Common Criteria Arrangement on the Mutual Recognition of Common Criteria Certificates in the Field of Information Technology Security* (CCMRA) was signed by the United States, Canada, France, Germany, and the United Kingdom to affirm their commitment to this goal. Both NIST and NSA signed the CCMRA on behalf of the United States.

The CCMRA identifies several conditions necessary for mutual recognition that include use of the CC and CEM as the basis for evaluation criteria and evaluation methods respectively, minimum requirements for Certification/Validation Reports, and the existence of a national Evaluation and Certification/Validation Scheme. To further the goal of achieving consistent, credible and competent application of the CC and CEM, the CCMRA also requires the Validation Body to monitor all evaluations in progress within its Scheme. It also requires the Validation Body to

establish procedures to ensure that Validation Body and the CCTLs affiliated with the Validation Body perform evaluations impartially; apply the CC and CEM correctly and consistently; and adequately protect the confidentiality of proprietary or sensitive information.

The CCMRA also requires that the Validation Body either be accredited by a recognized Accreditation Body in accordance with ISO/IEC Guide 65, *General Requirements for Bodies Operating Product Certification Systems (*ISO Guide 65) or be established under laws, statutory instruments, or other official administrative procedures valid in the country to meet the requirements of ISO Guide 65. The Validation Body has been established under the official administrative procedures of NIST and NSA to meet the requirements of ISO Guide 65.

The CCEVS is designed to meet both the intent of the CCMRA, and to further the goal of the United States Government in supporting the trustworthiness of IT products that are part of the national information infrastructure in the public and private sectors. The Validation Body, which is described in this document, is the organization established by NIST and NSA to implement the CCEVS. The CCEVS is described in Scheme Publication #1*, Common Criteria Evaluation and Validation Scheme*, *Organization, Management and Concept of Operations.*

[CCMRA Article 4, Annex B.2]

1.2 Purpose

This document satisfies the CCEVS requirement for a quality manual that includes the procedures demonstrating that the Validation Body complies with the requirements stated in Annex B of Scheme Publication #1*, Common Criteria Evaluation and Validation Scheme*, *Organization, Management and Concept of Operations*. All Validation Body standard operating procedures are either contained in this document or referenced in other CCEVS documents (see Annex B for titles). This is a living document and will mature as CCEVS policy and procedures develop. The SOP will be reviewed periodically and updated accordingly.

The primary audience of this document is the Validation Body staff. Others that may find it useful include members of a CCTL staff, security target (ST) and protection profile (PP) authors, product developers, and sponsoring organizations.

[ISO65 4.8.1c]

1.3 Organization of this Document

This document consists of the following nine chapters and six Annexes that describe the operating procedures for the Validation Body. At the end of each section is a notation in brackets, i.e., [ISO65 4.8.1c] which denotes the reference (ISO65, MRA, Scheme) to which we are compliant.

- Chapter 1 provides the background and context of the Validation Body
- Chapter 2 provides a general overview of the Validation Body
- Chapter 3 describes the Validation Body quality system
- Chapter 4 describes the Validation Body's quality management procedures
- Chapter 5 describes the Validation Body's resource management procedures
- Chapter 6 introduces the Validation Body's technical oversight and validation of security evaluations
- Chapter 7 discusses the procedures for data & records management
- Chapter 8 discusses the Validation Body role in the administration of Common Critieria evaluation laboratories within the CCEVS

- Chapter 9 describes the Certificate Maintenance Program
- Annex A contains a Glossary of Terms
- Annex B contains a list of CCEVS publications
- Annex C provides CCEVS contact information
- Annex D identifies Validation Body staff
- Annex E contains a list of approved Validation Body subcontractors
- Annex F contains a sample Non-Disclosure Agreement

1.4 References

Scheme Publication #1, *Common Criteria Evaluation and Validation Scheme, Organization, Management and Concept of Operations,* Version 2.0, dated May 1999.

Common Criteria for Information Technology Security Evaluation, Version 2.1, dated August 1999.

Common Evaluation Methodology for Information Technology Security Evaluation, Version 1.0, CEM 99/045, dated August 1999

Common Criteria Arrangement on the Mutual Recognition of the Common Criteria Certifications in the Field of Information Technology Security, dated October 5, 1998

ISO/IEC Guide 65, *General Requirements for Bodies Operating Product Certification Systems*, dated 1996

NIST Handbook 150, *Procedures and General Requirements,* dated March 1994

NIST Handbook 150-20, *Information Technology Security Testing—Common Criteria* Draft, Version 1.1, dated April 1999

1.5 Document Maintenance

The Validation Body maintains this document, as well as the other documents issued by the CCEVS. Page changes, addendums, or updated versions will be posted to the CCEVS website at the location indicated in Annex C.

[ISO65 4.8.2]

2 Validation Body Overview

The Validation Body is a government entity responsible for implementing the United States Common Criteria Evaluation and Validation Scheme (CCEVS) for Information Technology Security. The Validation Body was established under the following authorities:

a. Public Law 100-235, Computer Security Act of 1987
b. National Information Assurance Partnership (NIAP) Letter of Partnership National Security Agency and National Institute of Standards and Technology, dated 22 August 1997
c. NIAP Letter, Establishment of National Voluntary Laboratory Accreditation Program (NVLAP) Laboratory Accreditation Program (LAP) for Information Technology (IT) Security Testing, dated 5 August 1998
d. *Common Criteria Arrangement on the Mutual Recognition of Common Criteria Certificates in the Field of Information Technology Security*, dated 5 October 1998

In implementing the CCEVS, the Validation Body operates in accordance with the Scheme Publication #1*, Common Criteria Evaluation and Validation Scheme*, *Organization, Management and Concept of Operations;* ISO/IEC Guide 65 – *General Requirements for Bodies Operating Product Certification Systems;* and the CCMRA.

The responsibilities of the Validation Body are:

- To establish and implement policies and procedures for the operation of CCEVS. [Scheme 3.2]
- To communicate information about the CCEVS to the public. This includes information about the CCEVS, the Validated Products List, the Approved CCTLs List, and forms and instructions for participating in CCEVS activities. [CCMRA C.11, CCEVS 3.2]
- To assure that Validation Body services are provided to all qualifying organizations equally, without discrimination or undue financial hardship, and that the interests of all parties participating in CCEVS activities are given appropriate consideration. [Scheme 3.2, CCMRA C.1, ISO65 4.1.2]
- To approve CCTLs for participation in the CCEVS, provide test methods, technical guidance, and Government oversight to each evaluation, and monitor CCTL activities as they relate to the CCEVS. [Scheme 3.2]
- To review the Evaluation Technical Reports prepared by the CCTLs to verify that conclusions reached are consistent with the evidence presented, and provide a validation report for each evaluation completed under the CCEVS. [Scheme 3.2, 5.2]
- To issue CC Certificates to Sponsors whose products or PPs have been evaluated to conform to CC requirements according to the CCEVS. [Scheme 3.2]
- To implement measures to ensure that proprietary information entrusted to the Validation Body is not revealed to unauthorized parties. [Scheme 3.2]
- To promote the integrity of the certificates issued and correct use of the CC and NIAP logos. [Scheme 3.2, CCMRA C.9, C.14, C.15]
- To perform arbitration for all disputes that arise in the context of the scheme and provide procedures for appeal or conciliation. [Scheme 3.2, CCMRA C9i, C.12]
- To maintain a record system for creating, storing, accessing, archiving and disposing of Validation Body records used to document Validation Body activities.

[ISO65 4.2g, CCMRA Article 4, Annex C.3, CCEVS Annex B]

2.1 Validation Body Management

A Director and Deputy Director are selected by NIST and NSA management to control the activities of the Validation Body. The names and qualifications of the Director and Deputy Director as well as other key Validation Body personnel are included in Annex D. The Validation Body Director reports to the NIAP Director for administrative and budgetary matters and to the NIST and NSA certificate-issuing authorities for CCEVS operational matters. The certificate issuing authorities are the Director NIST, Information Technology Laboratory, and the Deputy Director for Information Systems Security, NSA or their designed representatives.

Validation Body management depends on the certificate issuing authorities for final decisions on issuance and revocation of CC certificates, for official signatures on CC certificates, for changes in Validation Body policy and for resolution of issues that involve interaction with the CCMRA partners. In that the certificate issuing authorities' primary function with respect to this document is signing of CC certificates, they are referred to as signatories throughout the rest of this document.

[ISO65 4.2b, 4.2c]

2.2 Validation Body Personnel

The Validation Body employs both technical staff and administrative support staff in order to provide the full range of services defined by the CCEVS. The Validation Body entrusts the accreditation of CCTLs to NVLAP and depends on the CCTLs for the evaluation of products and PPs. The Validation Body may contract portions of the Validation and Technical Oversight functions to organizations that have no financial or legal interests in the outcome of the validations.

All employees, contractors and others that provide services to the Validation Body via other arrangements are bound by the policies, procedures and other conditions set by the Validation Body and described in this document. Adherence to these policies and procedures is a condition of employment or of any other Validation Body agreement entered into with any other person or organization. Any deviation from these policies, procedures and other conditions, without the written consent of the Validation Body Director is grounds for employee dismissal or termination of the contract or agreement.

[ISO65 2.1, 4.5.3]

2.3 Validation Body Organization

The Validation Body is organized to effectively meet the goals of the CCEVS and assure the implementation of the Validation Body policies. The organizational chart is depicted in Figure 2.1.

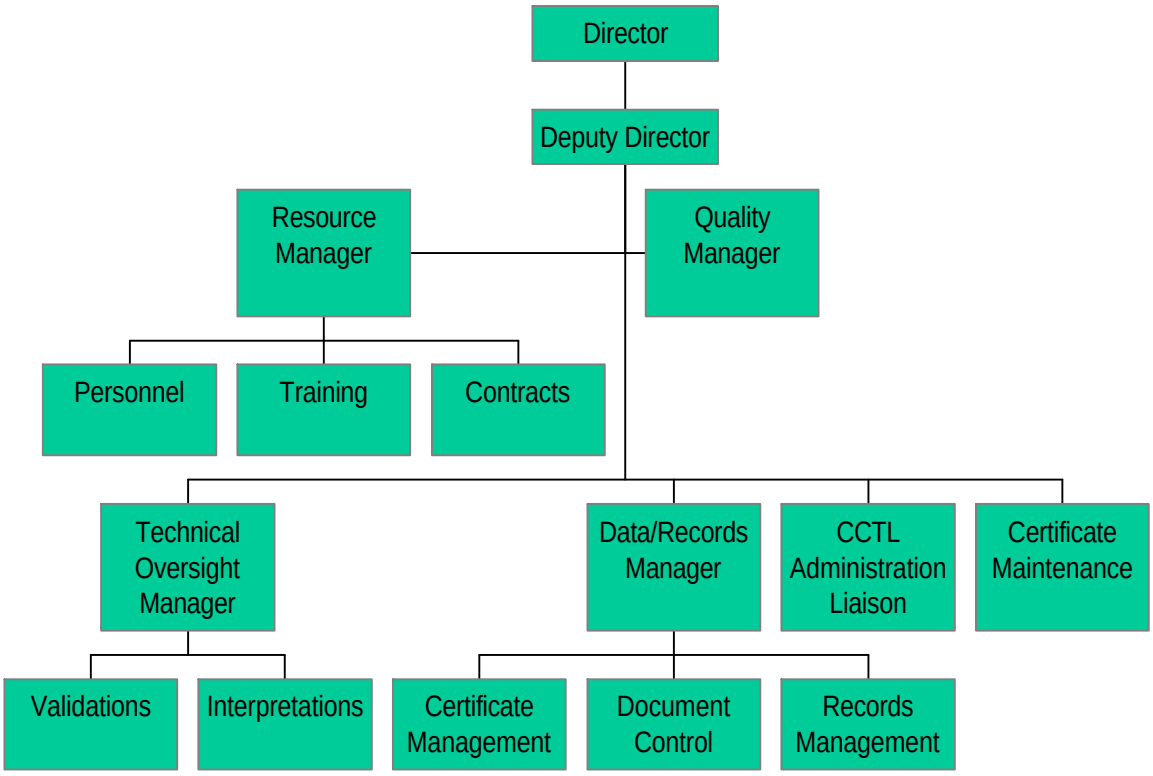

Figure 2.1

2.4 Funding Source

NIST and NSA are responsible for providing sufficient resources for the Validation Body to carry out its assigned responsibilities. For the first two years of operation, funding for the Validation Body will be provided by NIAP. At the end of two years, the Validation Body will evaluate the feasibility of transitioning to a fee for service operation.

[CCMRA C.3, ISO 65 4.2h,i, 4.8.1d]

2.5 Legal Status

NIST and NSA are the entities responsible for any contracts or binding agreements entered into by the NIAP CCEVS Validation Body, and for all actions performed by the Validation Body and its employees.

[CCMRA C.3d, C.9, ISO 65 4.5.3b, CCEVS Annex B]

2.6 Complaints and Appeals

Persons or organizations affected by Validation Body decisions and actions have the right to lodge a formal complaint and appeal the decision when they believe that Validation Body actions have not been conducted according to the rules or standards of the CCEVS or the actions have resulted in unfair treatment of persons participating in or are affected by Validation Body activities. A person or organization disagreeing with the Validation Body's decision on a complaint may appeal the decision for review by Validation Body management.

In resolving complaints and appeals the Validation Body may enlist the guidance of technical, regulatory and other relevant experts when necessary or form an independent arbitration panel to

resolve the dispute. Procedures for filing and resolving complaints and appeals are included in Section 4.6.

[ISO65 4.2p, 4.5.3k,m, 4.8.1f, 7.1, *CCEVS,* 3.2]

2.7 Public Information Dissemination

The Validation Body will make information about its operation and services available to the public. All CCEVS information for public consumption to include changes to validation requirements will be published and distributed to the public prior to the effective date of the change using the procedures described in Section 7.2, Document Control. The Validation Body Director or designee must approve all information about CCEVS activities before it is disseminated to the public. Information about contacting or retrieving information from the CCEVS may be found in Annex C. The list of publications available to the public is included in Annex B.

[ISO65 4.8.1, CCMRA C.11, CCEVS Annex B]

2.8 CCMRA Participation

The Validation Body's standard operating procedures have been developed to satisfy its CCMRA obligations. This includes:

- Acceptance of definitions defined in the CCMRA
- Co-development and adoption of common test methods and interpretations
- Providing Validation Reports and other CCEVS information to CCMRA participants
- Requesting CCEVS evaluated products to be added to CCMRA participants Validated Products Lists
- Adding products evaluated by CCMRA participants to the CCEVS Validated Products List
- Protection of proprietary information obtained from CCMRA participants

[CCMRA]

3 Validation Body Quality System Overview

The Validation Body Quality System is designed to ensure the provision of security evaluation and validation services for both government and industry that meets the quality and functional requirements of the CCEVS and of ISO Guide 65. The major components of the Quality System include policy, personnel organization and functional organization. Section 3.1 identifies Validation body policies. Section 3.2 describes the organization, roles, responsibilities and functions of the Validation Body personnel.

3.1 Validation Body Policies

In an effort to meet the requirements of the CCEVS and to promote total quality management, the Validation Body has adopted policies that apply to all persons performing validation activities on behalf of the Validation Body. This section contains the Validation Body's Quality Policy, Information Confidentiality Policy and the Records Management Policy.

3.1.1 Validation Body Quality Policy

A quality policy defines the overall intentions and direction of an organization with regard to quality, and is endorsed and expressed by upper-level management. The Validation Body's quality policy is shown below.

- The Validation Body shall provide its services in a non-discriminatory manner.
- The Validation Body will provide services at a fair price that does not cause undue financial hardship to those seeking to receive a CC certificate for their product.
- The Validation Body will implement and maintain a quality system for the operation of the CCEVS that includes compliance with the requirements of both the *CCMRA*, as enumerated in the *CCEVS*, and ISO Guide 65.
- The Validation Body will implement procedures to assure the impartiality, objectivity, and integrity in all Validation Body activities.
- The Validation Body will implement procedures that assure consistency across all evaluations.
- The Validation Body will protect proprietary information.
- The Validation Body will implement procedures to ensure timely and accurate reporting of validation results to the public.
- The Validation Body will implement procedures to monitor the use of issued CC certificates, and will revoke CC certificates or pursue legal actions against those that abuse the privileges granted or bring embarrassment to the Validation Body by use of the certificate and privileges associated with the certificate.
- The Validation Body will assure the adequacy and relevancy of Validation Body skills and expertise.

[ISO65 4.1.1, 4.1.2, 4.2a,e,,j, 4.5.1, 4.5.3a, CCMRA C.2, C.4, C.9, CCEVS Annex C Quality Manual(a)]

3.1.2 Validation Body Information Confidentiality Policy

The Validation Body has the responsibility to ensure the confidentiality of information obtained in the course of Validation Body activities at all levels of the organization, including committees and external bodies or individuals acting on its behalf. The supplier of information is responsible for marking/labeling all proprietary information delivered to the Validation Body. Any information designated as proprietary must not be disclosed, copied, reproduced or otherwise made available in any form to any other person not acting on behalf of the Validation Body, firm, corporation,

partnership, association or other entity without the consent of the supplier, except as such information may be subject to disclosure under the Freedom of Information Act (5U.S.C 552).

The Validation Body will use its best efforts to protect information designated as proprietary from unauthorized disclosure. The Validation Body will not be liable for the disclosure of information designated as proprietary that, after notice to and in consultation with the supplier, the Validation Body determines that it may not lawfully be withheld or that a court of competent jurisdiction requires disclosed.

All persons performing work for the Validation Body are required to sign non-disclosure agreements avowing that they understand and will comply with the proprietary information confidentiality policy described above. This applies to both employees and contractors. A sample non-disclosure agreement may be found in Annex F.

[ISO65 4.10, 4.10.1, 4.10.2, CCEVS Annex B, CCMRA C.10]

3.1.3 Validation Body Records Management Policy

The Validation Body is responsible for maintaining accurate records to demonstrate that CCEVS procedures have been effectively fulfilled and to ensure the traceability, repeatability, and reproducibility of evaluations and validations. Records that are generated, modified, or deleted by either Validation Body personnel or by persons performing work for the Validation Body, must comply with the Validation Body Records Management Policy as documented below.

- Records should be clearly identified and traceable to the procedure(s) involved, or to the quality system activity they document
- Records should be filed, indexed, and maintained in a manner that provides for safe storage and ready access or retrieval
- Records should be an accurate and truthful representation of actual events, documented in a timely manner
- Records should be dated and signed by the person(s) generating or modifying the records as specified in the applicable procedures
- Personnel involved in collecting data for records should be provided instructions and training to the degree necessary to ensure that the records are generated correctly
- The Validation Body requires that any person or organization performing work for the Validation Body, will make those records dealing with evaluation or validation activities available to the Validation Body

[ISO65 4.9.1, 4.9.2]

3.2 Validation Body Quality System Functions

The basic functions of the Validation Body quality system are quality management, resource management, CCTL administration, technical oversight of evaluations, data/records management, and certificate maintenance. Each function is briefly described below.

3.2.1 Quality Management

The quality management function, described in Chapter 4, assures that the operating procedures for the Validation Body completely addresses the intended functions, are explicitly defined, and can be audited. It also includes implementation of the procedures defined for quality management which include periodic reviews of the quality policy for effectiveness and relevance, internal audits to assess adherence to the policy in all functional areas, arbitration, and reporting to Validation Body authorities on the performance of the quality system.

[ISO65 4.2k, 4.5]

3.2.2 Resource Management

Recruitment, hiring, and training, described in Chapter 5, includes procedures for recruiting and hiring Validation Body staff, and procedures for training the staff.

[ISO Guide 65 4.2j, CCEVS Annex B Quality Manual(d)]

3.2.3 Technical Oversight and Validation

The Validation Body Technical Oversight and Validation function, described in Chapter 6, identifies procedures for performing validations, enforcing consistency across evaluations, and keeping accurate records to ensure traceability, repeatability, and reproducibility of evaluations.

[ISO65 4.3, CCEVS Annex B Quality Manual(f)]

3.2.4 Records Management

Data/Records Management, described in Chapter 7, includes procedures for creating, storing, accessing, archiving and disposing of Validation Body records that are used to document Validation Body activities.

[ISO Guide 65 4.9.1, CCEVS Annex B, Records]

3.2.5 Document Control

Document Control, described in Chapter 7, includes the procedures for approving, distributing, maintaining, and listing CCEVS documents and data.

[ISO Guide 65 4.8.2, CCEVS Annex B Document and Change Control]

3.2.6 Certificate Management

Certificate management, described in Chapter 7, includes procedures for issuing CC certificates, recognizing certificates by CCMRA partners, maintaining a Validated Products List, monitoring certificate use, revoking CC certificates, and maintaining certificates over the lifecycle of a product.

[ISO 65 12, 13, 14, 15, CCEVS Annex B Quality Manual(g)]

3.2.7 CCTL Administration/Liaison

CCTL Administration, described in Chapter 8, includes procedures for approving CCTLs, extending or reducing the scope of accreditation, renewal of CCTL approval, withdrawal or suspension of approval, informing the community of CCTL changes, audits, and validator observations.

[ISO65 4.3]

3.2.8 Certificate Maintenance

Certificate maintenance, described in Chapter 9, includes procedures for performing certificate maintenance, acceptance, monitoring and product re-evaluation.

4 Quality Management

The CCEVS requires the Validation Body to operate and maintain quality in CCEVS evaluations and certificates. To accomplish this the Validation Body has designated a Quality Manager, developed quality documentation, procedures for internal audits, management reviews, subcontractor management, and established an arbitration process for internal and external issues. Each of these quality elements is described below.

[ISO65 4.2k, 4.5.3h]

4.1 Quality Manager

The Quality Manager has the authority for ensuring that Validation Body policies are implemented and maintained in the Validation Body. The Quality Manager is responsible for:

- Ensuring that all personnel understand their role in achieving quality in the Validation Body
- Maintaining quality documentation
- Organizing and coordinating internal audits
- Coordinating management reviews of the Validation Body quality system
- Reporting on the performance of the quality system to Validation Body management
- Tracking and monitoring the status of complaints, disputes, and appeals, and corrective and preventive actions

[ISO Guide 65 4.5.2]

4.2 Instilling Quality in Validation Body Personnel

The Quality Manager is responsible for ensuring that all personnel are equipped to carry out their individual roles according to the Validation Body's quality system. To accomplish this the Quality Manager:

- Ensures that all personnel meet the qualifications of their assigned roles
- Provides periodic Validation Body Standard Operating Procedures training courses and seminars for personnel
- Ensures that all quality documentation is available to all personnel at the location(s) defined in Annex C

4.3 Quality Documentation

The Validation Body has documented its quality system and made the documentation available to all validation body staff members at the location(s) defined in Annex C. The Quality Manager is responsible for periodic audits and reviews (at least annually) to ensure that the quality documentation is understood implemented, and maintained according to the document control procedures in Section 7.2.

[ISO Guide 65 4.5.1, 4.5.2, 4.5.3(h)]

The Validation Body quality system documentation consists of:

Scheme Publication #1, *Common Criteria Evaluation and Validation Scheme for Information Technology Security—Organization, Management, and Concept of Operations*

Scheme Publication #2, *Common Criteria Evaluation and Validation Scheme for Information Technology Security—Validation Body Standard Operating Procedures*

Scheme Publication #3, *Common Criteria Evaluation and Validation Scheme for Information Technology Security—Technical Oversight and Validation Procedures*

Scheme Publication #4, *Common Criteria Evaluation and Validation Scheme for Information Technology Security—Guidance to Common Criteria Testing Laboratories*

Scheme Publication #5, *Common Criteria Evaluation and Validation Scheme for Information Technology Security—Guidance to Sponsors of IT Security Evaluations*

Scheme Publication #6, *Common Criteria Evaluation and Validation Scheme for Information Technology Security—Certification Maintenance Program*

NIST Handbook 150, *Procedures and General Requirements*

NIST Handbook 150-20, *Information Technology Security Testing—Common Criteria*

4.4 Internal Audits

The Validation Body has established the following activities for performing internal audits of its own quality procedures. The purpose of identifying these activities is to ensure that all internal audit activities are performed in a consistent manner, that audit results are adequately reported, and that any follow-up activity or corrective actions are taken.

Validation Body auditing activities include the following:

1. The Quality Manager, or designee, will develop and update an internal audit schedule to perform an audit of each quality system function at least once annually. The purpose of the audit is to verify that the Validation Body continues to comply with its quality system procedures. The schedule will contain the date of the audit and the function of the Validation Body to be audited. Ad-hoc audits can be scheduled based on identified problems by employees, external input, or for corrective actions.

2. For each audit, the Quality Manager will:

    - Identify or review previously identified objectives or goals for each audit
    - Establish an audit team and designate a team leader
    - Develop an audit checklist format and provide assistance to audit team leaders in developing specific checklist items for each audit
    - Ensure that each audit is conducted according to Validation Body procedures and as scheduled

3. Auditor(s) shall be properly trained and verified to be free from conflicts of interest with the target of the audit. In preparation for the audit, auditor(s) shall review the audit objectives,

the relevant quality system procedures, and any other information that would be helpful in conducting the audit.

4. Auditor(s) will notify the Validation Body Functional Manager(s) potentially affected by the audit one week prior to initiation of the scheduled audit. (note: ad-hoc audits will not provide a notification)

5. On the first day of the audit a meeting shall be held with the appropriate Functional Manager(s) to explain the objectives and procedures of the audit.

6. Audit findings will be recorded in an audit report. The audit report shall contain all findings and observations made by the auditor(s). Draft and the final versions of audit reports will be given to the Quality Manager and appropriate Function Manager(s) for review and distribution.

7. An exit meeting will be held with those involved in the audit to convey the findings of the audit.

8. The results of the audit and exit meeting will be documented in the audit report and the audit report will be placed under Validation Body records control for a period of five years. All corrective actions or other follow-up activities identified in the audit report will be coordinated with the Quality Manager, or designee.

[ISO Guide 65 4.5.3n, 4.6, 4.7.1]

4.5 Management Reviews

The Validation Body conducts two types of management reviews for quality: Program Area Management Reviews and Validation Body Management Review.

Program Area Management Reviews are reviews conducted within the Validation Body for a specific activity, e.g., training or document control. Program Area reviews are either mandatory or voluntary reviews. Mandatory reviews occur as part of the Quality Manager's quality system review schedule, whereas voluntary reviews are conducted by the appropriate Functional Manager to determine the status of quality for an individual activity.

A Validation Body Management Review covers the entire Validation Body as a single entity, drawing on the results of Program Area Management Reviews.

4.5.1 Program Area Management Review

A Program Area Management Review is conducted in a systematic manner using a formal agenda. The review agenda should include the following, as appropriate:

- Evaluation of results of internal audits or audits conducted by other bodies
- Evaluation of complaints received since last management review
- Evaluation of corrective action activity since last management review
- Results from any customer surveys conducted or other customer feedback
- Assessment of need to update Standard Operating Procedures
- Matters arising from the previous review
- Adequacy of Validation Body staff and equipment
- Staff training
- Development of corrective actions (if a need is identified during the review)

Actions arising from the review are documented by the program area review designee, assigned to the Functional Manager of the area where the problem or nonconformance exists and, preferably, are assigned a completion date by the Functional Manager or the Quality Manager. The results of management reviews are documented by the review board designee and placed under Validation Body document and records control for a period of five years.

[ISO Guide 65 4.5.3f]

4.5.2 Validation Body Management Review

The Validation Body management will establish a Validation Body Quality Review Board (VBQRB) that performs a formal evaluation of the Validation Body's quality system and quality policy.

The VBQRB will hold management review meetings at least annually. Minutes from each meeting will be prepared and distributed by the review designee to all VBQRB members within one week following the meeting. VBQRB meetings will address but are not limited to a review of:

- The Quality Policy and other quality documentation
- Quality System
- The organizational structure and quality infrastructure
- Feedback surveys
- Training plans
- Personnel reviews
- Internal audit results
- Program area management reviews
- Nonconformity/deficiencies and preventative/corrective actions
- Identification and prioritization of upcoming audits
- Next fiscal years plan of action

VBQRB minutes and any related documents will be placed in Validation Body document and records control for a period of five years by the review board designee.

[ISO Guide 65 4.5.3f, 4.7.2]

4.6 Complaints and Appeals

The Validation Body provides a process for dealing with complaints and appeals that originate either internally or externally. The process applies, but is not limited to:

- CCEVS actions, decisions, approvals or staff assignments,
- Validation Body customers and consumers,
- Internal quality system problems that may be detected by CCEVS staff members,
- CCTLs, candidate CCTLs, CCTL customers, or
- Unresolved issues that occur during PP or product evaluations

The Director of the Validation Body is responsible for ensuring that all complaints and appeals are responded to promptly and that corrective actions, if required, are implemented.

[ISO6 4.2p, 4.8.1f, 5 4.2p, 4.8.1f, 7.1, 7.2]

4.6.1 Complaints

Complaints are written expressions of dissatisfaction regarding the quality of the Validation Body's services provided to external or internal customers, or a claim that either the Validation Body or a

CCTL has acted incorrectly. Written complaints shall be submitted to the Director of the CCEVS Validation Body.

The Validation Body performs the following when a complaint is received:

1. Places the complaint under Validation Body document control and records management

2. Assigns the complaint a reference number and records the date of receipt

3. Forwards a copy of the Complaint Record to the Quality Manager for review and processing

4. Forwards a copy of the Complaint Record to the appropriate Functional Manager who is responsible for the program or operational activity identified in the complaint

If the complaint is not judged to be the result of a serious nonconformity, the Quality Manager notifies the complainant that no action is being taken and informs the complainant of his right to appeal.

If the complaint is judged to be a potentially serious nonconformity, the Quality Manager:

1. Issues a request for investigation and necessary corrective action to the responsible Functional Manager

2. Notifies the complainant that action is being taken

The Functional Manager to whom the complaint is assigned performs the following:

1. Investigates the complaint

2. Seeks the aid of independent and impartial technical experts to help resolve technical disagreements

3. Establishes a plan and actions to resolve the complaint

4. Reviews the plan and actions with the Quality Manager

5. Updates the plan and actions based on suggestions from the Quality Manager

6. Notifies the complainant of the planned decision and actions for resolving the complaint

7. Implements the actions to resolve the complaint

8. Notifies the Quality Manager when the complaint is resolved

9. Forwards copies of the response and any other documentation pertaining to the resolution of the complaint to the Quality Manager

10. The Quality Manager reviews the complaint resolution and decides to close the complaint or to request further action from the Functional Manager

11. When the complaint is closed, the Functional Manager responds to the complainant in writing within three days

12. After the complainant has been notified, all documentation and records pertaining to the complaint resolution are forwarded to the Quality Manager who places the complaint documentation under Validation Body document and records control

[ISO65 4.2p, 4.5.3m, 4.8.1f]

4.6.2 Appeals

If a complainant disagrees with the Validation Body's decision on a complaint, and is unsuccessful in achieving an acceptable reconsideration of the issue, the complainant may file a formal appeal.

All appeals are made in writing to the Director of the Validation Body within 30 days after notification of a Validation Body decision. In response to the appeal, the Validation Body performs the following:

1. When the Director receives an appeal of a complaint decision, a copy of the appeal documentation is forwarded to the Validation Body Quality Manager who places the appeal documentation in Validation Body document and records control for a period of five years. In developing a decision the Director may enlist the guidance of technical, regulatory and other relevant experts when necessary, or may form an independent arbitration panel. The Director has 30 days to reach a decision on the appeal.

2. Upon reaching a decision, the Director notifies the appellant in writing of the outcome of the appeal and forwards a copy of the decision and notification to the Validation Body Quality Manager. The Quality Manager places the decision in Validation Body document and records control for a period of five years.

3. If the appellant does not agree with the Director's decision, a re-appeal may be made in writing to the Director who will forward it to the NIAP Signatories for resolution. In developing a resolution the NIAP signatories may enlist the guidance of technical, regulatory and other relevant experts when necessary, or form an independent arbitration panel for a resolution. The NIAP Signatories have 30 days to reach a decision.

4. When an appeal is submitted to the NIAP Signatories, a copy of the appeal documentation is forwarded to the Validation Body Quality Manager who places the appeal documentation in Validation Body document and records control for a period of five years.

5. Upon reaching a final decision, the NIAP Signatories notify the appellant in writing through the Director of the Validation Body of the outcome of the re-appeal. A copy of the resolution and notification will be forwarded to the Validation Body Quality Manager. The Quality Manager places the decision in Validation Body document and records control for a period of five years.

6. A written copy of the resolution is sent to the appellant and is considered final.

[ISO65 4.2p, 4.8.1f]

4.7 Quality Management Records

This section lists the records required to support the traceability and integrity of the Quality Management procedures.

4.7.1 Quality Manager Records

- Statement of who the quality manager is

4.7.2 Instilling Quality Records

- Training course, seminar description and notice form

4.7.3 Quality Documentation Records

- Quality document list
- Quality documents

4.7.4 Internal Audit Records

- Audit schedule
- Audit objectives and checklist for each audit
- Audit team list and verification of freedom from conflict of interest
- Audit notification form
- Audit report
- Audit exit meeting findings report
- Document and record control forms for appropriate items

4.7.5 Management Review Records

- Quality Committee member list
- Review schedule
- Review meeting notification with agenda
- Review meeting minutes
- Document and record control forms for appropriate items

4.7.6 Complaint and Appeal Records

- Complaint
- Complaint decision
- Complaint decision notification
- Corrective action
- Appeal
- Appeal decision
- Appeal decision notification

5 Resource Management

The employed staff for the Validation Body are composed of NIST and NSA personnel. As such the Validation Body will coordinate with the respective NIST and NSA organizations' personnel offices in processing recruitment, hiring and training actions. All Validation Body Functional Managers will work with the Validation Body Personnel Managers to ensure that Validation Body policies and needs for recruitment, hiring and training are met, and duly coordinated with the respective NIST and NSA personnel offices.

5.1 Personnel

Each Functional Manager is responsible for defining recruitment and hiring needs to meet Validation Body staffing requirements, and for ensuring that the staff have the appropriate facilities to perform in their assigned roles. Along with meeting technical and managerial requirements, all candidate Validation Body personnel must agree to follow the policies of the Validation Body (e.g., be fair and impartial, protect proprietary information, and avoid conflict of interest).

Each Functional Manager completes the following activities for recruitment and hiring:

1. Specify and approve technical requirements for recruitment
2. Prepare and approve written criteria for recruitment
3. Identify potential candidates
4. Evaluate candidate applications, and determine candidate ranking
5. Select best qualified candidate
6. Provide written notification of selection to candidate
7. Arrange for hiring/reassignment of candidate
8. Ensure that newly assigned personnel sign non-disclosure agreement and conflict-of-interest forms
9. Ensure that newly assigned personnel is given a copy of their Validation Body role
10. Ensure that newly assigned personnel is given the necessary facilities to carry out the responsibilities described in their Validation Body role

[ISO65 4.2j, 4.5.3i 5.1.2, 5.2.2, CCMRA C.7]

5.1.1 Qualifications of Validation Body Roles

This section identifies the personnel qualifications required to fulfill Validation Body roles. At present only the Validator role is defined. Other Validation Body roles will be defined in a future version of this document.

5.1.1.1 Validator Qualification Requirements

Each individual involved in validation activities will be designated as a Validator Trainee, Validator, or Senior Validator. Within the designation of Validator, individuals will be further defined by class, where each Evaluated Assurance Level (EAL) will represent a class of validator.

Since the EALs are hierarchical, once a Validator obtains a class they will receive credit for all EALs beneath that class (i.e., a Class 4 (EAL 4) Validator can handle any class of evaluation, 1,2,3 or 4 where a Class 2 (EAL 2) Validator can only handle an EAL 1 or 2 evaluation). To obtain a class a Validator must have participated as a validator trainee in a successful validation effort for that EAL or provide evidence of equivalent experience.

The minimum requirements for each validator designation are:

1. Validator Trainee
   - Completed ND284 Designing a Protection Profile
   - Completed CEM Training Course
   - Participated in at least one evaluation effort

2. Validator
   - Certified as a Validator Trainee
   - Participated in at least 2 evaluations (one of which must be a criteria-based evaluation)
   - For each class of Validator (EAL 1, 2, 3, 4) participated as a Validator Trainee in two validation efforts at a given level or higher. (NOTE: EALs are hierarchical therefore participation at a higher level gives credit for lower levels)

3. Senior Validator
   - Certified as a Class 3 Validator
   - Validated at least one Protection Profile Evaluation
   - Participated as an Evaluator in 3 evaluations (one of which must be at EAL 1 or 2 and another at EAL 3 or 4 or equivalent and must be in at least two different technologies)

[ISO65 5.1.1, 5.2.1, CCMRA C4.2]

5.2 Training

Each Functional Manager is responsible for making decisions regarding education and training requirements for their organizational functions and associated roles. Functional Managers are also responsible for developing and reviewing individual training plans annually for staff members for whom they are responsible.

Each Functional Manager completes the following activities for training:

1. Specify and approve training requirements for functional roles

2. Prepare an individual training plan and experience profile for staff members

3. Review training plans with staff members for whom they are responsible

4. Submit request to have training plan placed under document control

5. Monitor the implementation of the training plan

6. Update training plans and review with staff member

7. Submit request to have updated training plan placed under document control

[ISO65 4.2j, 5.2.3]

5.3 Contracts

The Validation Body assumes the responsibility for all technical decisions and work performed by or on behalf of the Validation Body. Any contracting or other agreement entered into between the Validation Body and any person or organization will be documented to include the arrangements of the agreement that includes adherence to Validation Body policies and procedures. The list of approved contractors is included in Annex E.

[ISO65 4.4, 4.5.3j, 5.2.2, CCMRA Article 11, Annex C.10, CCEVS Annex B]

5.3.1 Contractor Management

When the Validation Body determines a need to subcontract work, it will perform an assessment of potential contractors and establish a contract or working agreement with them. The Contracting Manager is responsible for all subcontracts and working agreements, and the assessment of contractors. Note that organizations performing work for the Validation Body through contracts or working agreements are all referred to as contractors.

The acquisition of contracted services will be done through the respective NIST and NSA organizations. As such the Validation Body will coordinate with the respective NIST and NSA organizations' procurement offices in processing procurement actions. The Validation Body Contracting Manager will ensure that Validation Body policies and contracting needs are met and duly coordinated with the respective NIST and NSA procurement offices.

5.3.2 Contractor Selection Criteria

Contractors will be selected based on their ability to satisfy Validation Body needs. Criteria to be used in selecting a contractor includes, but is not limited to:

- Conflict of Interest
- Evaluation experience
- CC and CEM experience
- Technical skills
- Quality Systems Experience
- Available resources

[ISO Guide 65 4.5.3(j); Scheme, Annex B Quality Manual (h)]

5.3.3 Contractor Assessment and Monitoring

All contractors are required to meet the Validation Body's quality system requirements. To ensure the contractor meets the requirements, they shall:

- Conform to the Validation Body's Standard Operating Procedures while performing Validation Body work
- Submit to audits and reviews as described in Sections 5.4 and 5.5

The activities the Validation Body may perform in monitoring a contractor depend on the details of the contract or working agreement and may include the following:

- Review status reports
- Review deliverables
- Review contractor audit reports

[ISO Guide 65 4.5.3(j); Scheme, Annex B Quality Manual (h)]

5.3.4 Contractor List

The Validation Body's approved contractors list is contained in Annex E.

[ISO Guide 65 4.5.3(j); Scheme, Annex B Quality Manual (h)]

5.4 Resource Management Records

This section lists the records required to support the traceability and integrity of the Resource Management procedures.

5.4.1 Recruitment and Hiring Records

- Requirements for candidate positions
- Candidate rankings
- Notification of selection letter
- Non-disclosure agreement
- Conflict-of-interest forms

5.4.2 Training Records

- Requirements for each role
- Training plans
- Experience profile
- Document control requests

5.4.3 Contractor Management Records

- Contract and working agreement
- Conflict-of-interest forms
- Contractor solicitation statement (which should include purpose, criteria, etc.)
- Contractor agreement to comply with Validation Body's SOP
- Contractor list
- Contractor deliverables, e.g. status report, audit reports

6 Technical Oversight and Validation

To achieve oversight activities the scheme will employ a validation program that is designed to combine training and practical experience to provide the breath and depth necessary to provide competent Validators to insure the quality of evaluation results produced by the scheme. An overview of the CCEVS Validation process is described below. Detailed procedures for administering technical oversight and validation are described in Scheme Publication #3, *Common Criteria Evaluation and Validation Scheme for Information Technology Security - Technical Oversight and Validation Procedures.*

6.1 CCEVS Validation Process

A sponsor of an evaluation (e.g., vendor of a product or protection profile developer) interested in obtaining a Common Criteria evaluation through the scheme approaches one or more of the CCEVS authorized CCTLs to solicit evaluation proposals. Any discussions regarding the price of the evaluation, the nature or conditions of payment, and the schedule for the evaluation are left entirely up to the CCTL and the sponsor of the evaluation. Similarly, proposal content and any screening or pre-investigation that the CCTL may wish to conduct regarding the viability of the protection profile or product is left to the discretion of the CCTL. When entering into an agreement with a customer the CCTL must ensure that there is no conflict of interest or appearance of conflict of interest in performing this evaluation if the intent is to obtain a CCEVS Certificate. Once the sponsor of the evaluation selects a CCTL and they have an agreement the CCTL must submit the evaluation for formal acceptance into the scheme[1]. In order for a product or system to be accepted into the scheme the CCTL must submit the following items to the Validation Body: 1) a complete Security Target for the Target of Evaluation (TOE), 2) an overview description of the TOE, 3) the name(s) of the vendor and CCTL POCs, and 4) a complete Evaluation Workplan for the evaluation. For a protection profile evaluation to be accepted into the scheme the CCTL must submit the following items to the Validation Body: 1) the complete protection profile, 2) the name(s) of developer/owner of the protection profile and the CCTL POCs, and 3) a complete Evaluation Workplan for the evaluation.

Once the Validation Body receives an application for evaluation acceptance from a CCTL the Validation Body will review the submitted information and identify validation resource needs for the effort within 2 business days. Based on this initial review of the ST or PP, EAL, and complexity of the TOE or PP, one or more validation personnel will be assigned and a Lead Validator designated. Additionally senior validation personnel from the Validation Body will be identified to provide support and guidance to the Validator(s) upon the request of the Validator. Within 8 business days of assignment, the Lead Validator for the evaluation will conduct a complete review of all information and using the ST or PP and evaluation workplan they will develop a Validation Plan for this evaluation. The Validation Plan will outline the various validation activities, validation milestones and their approval authority. The Lead Validator then presents the plan for Technical Oversight Manager concurrence.

The assigned validation personnel will then meet with the CCTL and Sponsor to review the evaluation and validation plans, identify validation milestones, and generally manage expectations. Once this meeting has occurred and all parties are in agreement, the Validation Body, CCTL, and Sponsor will sign an evaluation agreement stating the evaluation has been officially accepted into the scheme and all activities can commence.

[1] While it is envisioned that sponsors of evaluations and CCTLs will enter into an agreement before approaching the CCEVS Validation Body it is acceptable for the sponsor and/or CCTL to approach the CCEVS Validation Body prior to entering into a formal agreement to assess the feasibility of conducting an evaluation under the scheme. This pre-acceptance meeting will in no way replace the formal notification process and meeting necessary for formally entering into the scheme.

If a CCTL begins an evaluation without obtaining official acceptance into the scheme the Validation Body may refuse to offer validation services for that particular evaluation. Alternatively, the Validation Body may require all scheme procedural steps be done and the evaluation process may need to be re-started from the beginning in order for the Validator(s) to perform their functions.

After an evaluation has been officially accepted into the scheme the evaluation and validation activities will commence. The CCTL will conduct all evaluation activities in accordance with the CEM, the evaluation workplan, and CCEVS process. The Validator will concurrently monitor CCTL activities, conduct validation activities in accordance with the Validation Plan, prepare and submit validation status reports in accordance with the validation plan, coordinate all CCTL generated Observation Reports (ORs) submitted to the Validation Body, and provide continual interface with the Validation Body.

Upon completion of the evaluation the CCTL will provide the Validator with an Evaluation Technical Report (ETR) (as defined in CEM), all evaluation ORs along with any corresponding Observation Decisions (ODs), and a draft Validated Products List Entry Summary. After a detailed review of all information the Validator will produce a Validation Report and recommendation. The Validation Report and Validated Products List Entry Summary will concurrently be submitted to the CCTL and Sponsor for accuracy and release approval. Validators will provide a final recommendation to the Technical Oversight Manager for his concurrence and presentation to the Director of the Validation Body.

Using the final recommendation, the Director of the Validation Body will make the final decision to either 1) prepare a Common Criteria Certificate for signature, issue a Validated Products List Entry, and notify our Common Criteria partner schemes for mutual recognition; or 2) notify the CCTL and Sponsor of the unsuccessful completion of the evaluation and the rationale for this decision.

6.2 Interpretation Process Overview

A CCEVS interpretation board will be used to provide guidance for technical and process issues in CCEVS evaluations. The board receives issues needing clarification or formal interpretation from CCEVS management, validators, or the general public. The interpretation board drafts proposed statement of technical guidance, and facilitates the scheme and public discussion of draft interpretations to ensure that diverse views are considered. Once all views are considered and incorporated, as appropriate, the proposed interpretations are submitted to the Director, CCEVS for approval. Once approved, the interpretations are submitted to the CCIMB for international coordination. The details of the interpretation board operating procedures will be documented in a separate scheme document.

6.3 Technical Oversight and Validation Records

6.3.1 Validation Records

- CCEVS Evaluation Application Package from a sponsor and CCTL
- Documented review of the application package by the Validation Body
- Letter to sponsor and CCTL on readiness of product for evaluation
- Validation Body master schedule update
- Validator team list
- Status reports developed by validator, CCLT, vendor, and Validation Body
- Observation reports
- Validator monitoring or audit reports

- Validator progress reports for validator, CCTLs, and each evaluation
- Final ETR from the CCTL
- Draft Validation Report from the validator
- Schedule update request
- Final Validation Report
- Document the recommendation for the evaluation
- Document the observation decision tied to the observation report
- Letter to CCTL and sponsor to communicate the decision for the evaluation
- Update request to update the NIAP Validated Products List
- Letter to communicate validated product to CCMRA participants

6.3.2 Interpretation Records

- U.S. Interpretations Approval CCEVS Form 6001 and accompanying interpretation
- Interpretation Board meeting minutes

7 Data/Records Management

7.1 Records Management

A record is defined as a document that furnishes objective evidence of activities performed or results achieved. The Validation Body maintains a record system for creating and storing records to demonstrate that validation procedures have been effectively fulfilled, particularly with respect to application forms, evaluation reports, surveillance activities, and other Validation Body internal documents relating to granting, maintaining, extending, or withdrawing validation. The Validation Body also maintains records on CCTL accreditation and approval as well as records on internal Validation Body quality activities (e.g. audit reports). The Validation Body has established a set of procedures for working with the record system. These procedures apply to both paper and electronic records, and are identified in the following paragraphs.

[ISO65 4.9, CCMRA C6]

7.1.1 Responsibility for Records

1. The Director of the Validation Body is responsible for ensuring that all records are managed in conformance with the Validation body record policy identified in Section 3.1.3 and with the procedures identified in this section. Each Functional Manager is responsible for assuring that staff members maintain records documenting the activities associated with the function.

2. Each staff member that creates a record is responsible for ensuring that the record is correctly identified (identification of the record is a function of the type of record); the record is complete and legible and has been dated; all signatures and initials are filled in where necessary, the record content is clear, is correct and had not been improperly altered; and any errors have been properly corrected, initialed, and dated. All records that are proprietary must be clearly marked as such.

[ISO65 4.9.1, CCMRA C6, CCEVS Annex B]

7.1.2 Types of Records

Records will be generated and updated for activities performed by each of the functional organizations in the Validation Body. Folders, consisting of groups of records pertaining to a particular subject, will at a minimum, be maintained for each product evaluation, CCTL, person employed by the Validation Body, and each subcontract or agreement. Folders will be maintained on other subjects at the discretion of the Director. Copies of records may be stored in multiple record folders when it is relevant and useful. The types of records that are generated by each Validation Body function are described below.

1. Quality records are organized by quality function and provide objective evidence of the extent of fulfillment of the requirements for quality or the effectiveness of the operation. They include management review reports, corrective and preventive action records, internal audit records, subcontractor reviews, complaints, disputes, appeals, and results of arbitration.

2. Resource records are organized by employee name and includes hiring information, qualifications, training history, assignments and performance assessments related to CCEVS activities.

3. Technical Oversight records are organized by evaluation applicant and include the completed application and actions taken reviewing the application, correspondence regarding

acceptance or rejection of the application, plan for the evaluation that includes schedule and validators assigned, status reports, observation reports, audit reports, ETR, minutes of meetings and review, final validation report, validation decision and any other correspondence regarding the evaluation.

4. Data Management Records include document approvals, document distribution, document change notification, archiving of information, disposal of information, and access to proprietary or controlled folders of records.

5. CCTL Administration records are organized by CCTL and include information and correspondence regarding application, changing scope of accreditation, renewing accreditation/approval, withdrawal or suspension of accreditation/approval, CCTL audits, customer complaints and validator observations.

6. Certificate Maintenance records are organized by evaluation applicant and include information about certificate issue and delivery, certificate revocation, certificate maintenance activities, and surveillance activities.

7.1.3 Record Storage and Access

1. Each employee is given access to folders of records at the discretion of the functional manager responsible for the folder. The decision for granting access is based on the employee's job requirements.

2. All records that contain information of a confidential or sensitive nature must not be left on desks unattended, must be locked in office file cabinets when not in use, and must not be given to persons who have not been approved to view the data. Functional managers have the responsibility for checking work areas on a daily basis to assure that sensitive information is not left in the work areas unattended.

3. The Records Manager will control access to record folders based on access control lists that have been established by functional managers and approved by the Director. Each access to a folder with sensitive information will be logged.

4. A folder that contains records about a validation or CCTL must be signed out through the Records Manager when the folder is removed from its designated location.

5. For electronic folders, the server is configured to prohibit unauthorized access to server folders. The access permissions are set by the Records Manager based on access control lists that have been established by the functional managers and approved by the Director.

6. The Records Manager will perform backups of electronic records and folders on a scheduled basis.

[ISO65 4.9.1, CCEVS Annex B]

7.1.4 Archiving

All records pertaining to an evaluation must be kept for at least five years after the completion of the validation. This includes all records and other papers produced in connection with each validation. Other Validation Body records will also be archived and retained for five years or other period of time based on their type. The Records Manager is responsible for archiving information and for creating a record identifying the information being archived and the location of the archive.

[ISO65 4.9.1,4.9.2, CCMRA C6]

7.1.5 Disposal

1. All non-proprietary records supporting an evaluation will be destroyed after the archive period has expired.

2. All other proprietary information stored on behalf of a sponsor must be returned to the entity unless the entity gives the Validation Body other directions. A record documenting this transfer of information will be kept.

3. The Records Manager is responsible for proper disposal of information once approval has been obtained from the Director. Paper records will be shredded. Electronic records will be erased using a utility that conclusively overwrites the information. The Records Manager is responsible for creating a record of the disposal activity.

[ISO65 4.9.2]

7.1.6 Retention of E-mail Messages and other Electronic Submissions

1. Persons receiving E-mail messages that contain substantive information that is necessary to adequately and properly document the activities and function of the Validation Body must print the message and file it with other records that apply to the same subject.

2. WWW transactions that contain substantive information that is necessary to adequately and properly document the activities and function of the Validation Body must be printed out and filed with other records that apply to the same subject. The Validation Body person that effects the transaction is responsible for filing this information.

3. In deciding whether a particular message or WWW transaction is appropriate for preservation, employees should exercise the same judgment they use when determining whether to retain and file paper records. When in doubt, the person's supervisor should be consulted.

[ISO65 4.9.1]

7.1.7 Records Management Records

To assure the traceability and integrity of the Records Management functions, the following events will be documented and stored as official Validation Body records:

- Validation Body personnel access to proprietary information and records (date, who had access, what information or records were accessed)
- Written consent for disclosure or disposal of proprietary or sensitive information and records to a third party (date, why disclosure necessary, Validation Body person granting approval, third party consent)
- Disposal of information or records (date, who authorized disposal, identity of information or records)
- Movement of information or records to archive (date, who authorized move, identity of information or records)

7.2 Document Control

The Validation Body maintains procedures to control documents and data related to the CCEVS. This includes documents and data developed by Validation Body personnel to implement the

CCEVS, as well as documents and data supplied by CCTLs, sponsors, developers, and subcontractors. The procedures established for document control are document approval, document distribution, document maintenance, and document listing.

[ISO65 4.5.3g, 4.8.1, 4.8.2, CCMRA C5b]

In implementing these procedures, the Validation Body uses common document control identifiers for all documents and data. These common identifiers include:

- Document numbers: unique number assigned by the Validation Body for each publication or form
- Titles: each document has a unique descriptive title
- Author: each publication is assigned an author or editor
- Publication date: each publication is given an initial publication date. Effective dates are included where relevant.
- Revision dates: subsequent revisions are numbered and recorded
- Document addendums and/or page change addendums
- Sensitivity marking: all documents that are not intended for public distribution must be marked to include the restrictions on its distribution.

[ISO65 4.8.1, 4.8.2, CCMRA C5b] [ISO65 4.10]

7.2.1 Document Approval

Though the Validation Body Director is ultimately responsible for the technical and editorial quality of all documents and data prepared by Validation Body personnel, it is the Functional Managers and Quality Manager who have direct responsibility for ensuring quality in Validation Body documents and data.

7.2.1.1 Validation Body Director

1. Approve all documents and data that are published for external distribution
2. Ensure all documents and data that are published for external distribution are submitted to the Document Control Manager with instructions for distribution

7.2.1.2 Functional Managers

1. Identify the need for a document or data and obtain necessary resources
2. Review and approve documents and data which are specific to his/her assigned functional area
3. Ensure that documents and data are appropriately marked with the appropriate document control identifiers, e.g., proprietary, draft, obtained from the Document Control Manager
4. Ensure that all documents and data are free of routine errors
5. Ensure that all documents and data are reviewed and approved by the appropriate levels of authority prior to distribution

6. Ensure that all documents and data are submitted to the Document Control Manager along with a distribution list for record control

7.2.1.3 The Quality Manager

1. Ensure that quality system documents and data are reviewed and approved

2. Obtain appropriate approval signatures for quality system documentation

3. Ensure that quality system documents and data have document control identifiers obtained from the Document Control Manager and are assigned to the appropriate individual or functional area

4. Ensure that quality system documents and data are submitted to the Document Control Manager along with a distribution list for record control

7.2.2 Document Distribution

1. Documents and data are distributed according to their associated distribution information. The mechanisms for distribution include the Validation Body WWW site (reference Annex C), delivered to a CCEVS participant as a result of a validation activity, or mailed to the requestor by specific request.

2. To receive notification of documentation updates, the requestor must be on the document or data distribution list. An application will be available on the WWW as well as in paper format for this purpose.

3. When an applicant is accepted into the CCEVS, the Director will request that the relevant documents and data be forwarded to the applicant. The manager of Document Control will provide the requested documentation and will generate a record that documents the delivery of the documents and data. The manager will also add the applicant to the Validation Body mailing list so that the applicant will be notified of changes to the documentation. The date of the applicant inclusion on the list will also be recorded.

4. Employees, subcontractors and other persons performing work for the Validation Body may request document or data from the Document Control Manager using a Document Request form or may download them from the WWW site. The Functional Manager responsible for the request must approve any requests for Validation Body documents and data that are not releasable to the general public. Any distribution of controlled documents and data must be recorded.

5. All public requests for documents and data via mail or phone request will be forwarded to the Document Control Manager for processing. The Document Control Manager will keep a record of the request as well as a record of the information disseminated and the person or organization to which it was delivered.

[ISO65 4.8.1, 4.8.2, CCMRA C5a,d]

7.2.3 Document Maintenance

Changes to documents and data may occur as the result of a quality audit or review, or at the request of any Validation Body employee. If the document or data to be revised or issued is externally generated, the Validation Body employee contacts the generating organization, and will coordinate obtaining the new/revised document or data.

If the request is for a revision of the Quality System documentation or data the employee contacts the Validation Body Quality Manager. If the request is for the addition or revision of other Validation Body documents or data, the employee contacts the Functional Manager.

The Quality Manager and Functional Managers will adhere to the following procedures while maintaining documents and data:

1. Documents and data will be updated as necessary to reflect the requested change(s). The Quality Manager and Functional Managers will determine if the changes in documentation are required and will obtain the necessary resources to perform the change(s). An updated document requires the same review and approval as a new document. See the Document Approval section above.

2. The Document Control Manager will notify and distribute the updated documents or data as specified in the distribution information associated with the document or data.

3. Announcements of new or updated documents and data will also be posted to the Validation Body WWW site, see reference Annex C. This information will be posted within five days of approval of the new or updated documents.

4. Documents and data that are obsolete or have been superseded by a new document will be removed from the document list and will not be distributed by the Validation Body.

[CCMRA C5b, ISO65 4.8.1, 4.8.2]

7.2.4 Document Listings

The Validation Body will maintain a listing of all documents and data that it currently supports. It will also maintain a historical record of all documents that it has issued and will archive versions of older documents that are no longer in print. This archive will be maintained for at least the life of the Validation Body.

These listings will be updated by the Document Control Manager within three days after a new or updated document is issued. All CCEVS functional managers will be sent an updated document list within one week after the updated list has been approved for release by the Validation Body Director. The updated list will also be posted to the Validation Body WWW site in this same time frame.

[CCMRA C5b, ISO65 4.8.1, 4.8.2]

7.2.5 Document Control Records

This section lists the records required to support the traceability and integrity of the Document Control procedures.

- Document approval form
- Distribution instructions
- Request to Document Control Manager to list a document or data
- Request to be added or removed from a distribution list
- Request form to receive documents and data
- Document or data transmittal form
- Document or data change request

7.3 Certificate Management

The Validation Body issues Common Criteria certificates for products and PPs that have met the evaluation criteria under the CCEVS. A product or PP that has received a CC certificate is referred to in this document as a validated PP or product. Once a certificate has been issued, the Validation Body publishes a summary of the certificate information in the Validated Products List and promotes the integrity of CC certificates. [ISO65 4.8.1b, 12, 13, 14, 15]

7.3.1 Issuing a Common Criteria Certificate

CC certificates are issued to product developers, sponsors, or PP developers on behalf of IT products and PPs that have been evaluated and validated against the CC according to the rules of the CCEVS. To be valid, the certificates must be signed by both the NIST and NSA signatories. The certificate issued is valid only for the specific version and release of the product or the particular version of the PP identified on the certificate.

7.3.1.1 Certificate Issuing Procedure

1. Following the decision by the Director of the Validation Body to issue a CC certificate for a product, the Director prepares the proposed certificate along with rationale for issuing the certificate and forwards the certificate to the NSA and NIST signatories for signature. The contents of a CC certificate is described in Scheme Publication #1*, Common Criteria Evaluation and Validation Scheme*, *Organization, Management and Concept of Operations*, Annex E.

2. The CCMRA partners are notified of the certificate issue and are provided with the same information that is published in the Validated Products List.

3. Records are generated documenting the issuance of the certificate.

[ISO65 4.2f, 4.6, 4.6.1, 4.6.2a, 4.8.1c, 12.1, 12.3, 14.1, CCMRA Article 6, Annex C, Annex E, Annex J, CCEVS 5.3]

7.3.2 Recognition of CC Certificates Issued by CCMRA Partners

By signing the CCMRA, the United States has agreed to recognize the validations performed by the other nations that are party to the CCMRA. The following procedure is implemented to comply with this portion of the CCMRA.

7.3.2.1 Procedure for Recognition of CC Certificates Issued by CCMRA Partners

1. When information is received from an CCMRA partner about the issue or revocation of a CC certificate by the partner's validation body, the CCEVS Validation Body will review the issued certification/validation report and Security Target to assess whether the issued certificate clearly meets the requirements of the CC and the CEM and that the CCEVS Validation Body concurs with the conclusions reached.

2. If the CCEVS Validation Body concurs with the CCMRA partner's issued certificate the CC certificate information will be included on the CCEVS Validated Products List. If after the review of the report, it is recommended not to recognize the certificate of a partner the Director, CCEVS will submit the recommendation to NIST and NSA signatories for final approval. If the NIST and NSA signatories decide that the certificate will not be recognized then the Director of the CCEVS will send a letter to the submitting CCMRA partner notifying them of the nonacceptance of the certificate along with rational for why the certificate was not accepted. If the NIST and NSA signatories decide to accept the CCMRA partners' issued

certificate the CC certificate information will be included on the CCEVS Validated Products List.

If a notice of revocation of a CC certificate is received from a CCMRA partner the entry in the CCEVS Validated products list will be removed.

3. The information must be posted on the Validated Products List within 5 working days after the information is passed to the maintainer of the Validated Products List.

4. A CC certificate entry may be removed from the Validated Products List at the discretion of the NIST and NSA signatories in response to a recommendation from the Director.

[CCMRA Article 6, B.2h]

7.3.3 Maintaining a Validated Products List

The Validation Body will create and maintain a Validated Products List that identifies products and PPs that have been evaluated under the CCEVS, and products and PPs that have been evaluated under the Schemes of the CCMRA partners. The purpose of the Validated Products List is a) to provide information to the public about evaluated products that are available, and b) provide a source of reference for users to verify the current status of issued certificates.

For each product on the list evaluated under the CCEVS, the Validation Body will publish a copy of the certificate, identification of the Validation Body that has issued the certificate, and a copy of the Validation Report that must include the ST.

7.3.3.1 Procedure for Maintaining the Validated Products List

1. The maintainer of the Validated Products List, upon receiving information regarding a newly issued CC certificate, will format an entry that includes the certificate information, Validation Report, and the identification of the Validation Body that issued the certificate. In the event that the certificate has been issued as part of the CCEVS Certificate Maintenance Program, the entry will be appended to the already existing entry that documents the issuing of the certificate for an earlier version of the same product. A record of the updated action will be generated.

2. Upon receiving notice of certificate revocation, the maintainer of the Validated Products List will remove all summary information about the product from the Validated Products List and annotate the entry to note revocation of the certificate and effective date.

[ISO 4.8.1g, CCMRA Article 6, B.2h, CCEVS 3.2l]

7.3.4 Certificate Use Monitoring

The Validation Body will monitor the use of Common Criteria certificates for each CCEVS validated product to verify that suppliers adhere to the rules associated with the use of CC certificates. The holder of a certificate can use the certificate for any purpose as long as such use does not misrepresent or violate the intent or rules of the CCEVS or the CCMRA. These rules are listed below:

- Make claims regarding validation only in accordance with the CCEVS guidance given in Scheme Publication #5. See Annex B.
- Do not use the product validation in such a manner that would bring the Validation Body into dispute
- Upon revocation of a certificate, the certificate holder must immediately discontinue use of all advertising matter that contains reference to the product or PP evaluation

- Use the certificate only to indicate that products were evaluated and validated using the CC at the designated EAL
- Do not use the CC certificate or Validation Report in a misleading manner
- Follow the CCEVS guidelines for display of CC Certification Mark
- Inform the Validation Body of any changes to an evaluated product
- Keep records of all consumer complaints to the product developer or sponsor relating to the product's compliance with the CC
- Take appropriate action with respect to those complaints or disputes that affect compliance with the requirements for validation; this includes documenting the actions taken

7.3.4.1 Procedure for Monitoring

1. The Validation Body will respond to complaints from product users or any other source on issues regarding a specific product evaluation by examining examples of the product and product literature in question, communicating with the product developer regarding the issues, and initiating action if warranted.

2. All complaints and subsequent Validation Body actions will be documented as official records.

3. If the misuse of a certificate has been determined, the Validation Body will request that the perpetrator correct the misuse or may initiate administrative, procedural or legal steps to correct the misuse. The Validation Body may remove the product or PP from the Validated Products List upon determination of certificate misuse.

4. All monitoring activity must be documented in Validation Body records.

[ISO65 4.2g, 4.6, 4.6.1, 4.6.2a, 4.8.1e, 8.1.2a,c,d,e,f,g,h, 13, 14.1, 14.3, 15, CCMRA C.14 CCEVS Annex B, D]

7.3.5 Certificate Revocation

The Validation Body Director may recommend revocation of an issued CC certificate if the Validation Body determines that the product no longer meets the criteria for which it was validated or if the holder of the certificate violates the conditions for its use. A revocation may also occur at the request of the product developer who may not want to be bound by the responsibilities of a CC Certificate holder. As a result of revocation, the summary information about the validated product is removed from the Validated Products List and a notation is made of the revocation and effective date.

7.3.5.1 Revocation Procedure

1. The Validation Body Director will initiate revocation of a CCEVS issued CC certificate, based on evidence presented by Validation Body staff that conclusively demonstrates that the product no longer meets the criteria for which it was evaluated or the holder of the certificate has violated the conditions for its use.

2. The Validation Body Director will inform the certificate holder, by certified letter, return receipt requested, of the reasons for the proposed certificate revocation and the procedure for appealing the action.

3. If the certificate holder does not appeal the proposed revocation or correct the documented problem, the Validation Body Director will issue a final written decision 30 days after the date

of the revocation letter. If the certificate holder appeals the decision, revocation action is suspended until the appeal is resolved using the procedures described in Chapter 4.

4. If a certificate holder opts to correct an identified problem, the Validation Body will verify that the corrective action was appropriate and resolves the problem before withdrawing the revocation notice. The certificate holder will be given 30 days to correct the identified problem and present the evidence to the Validation Body. If the problem is not corrected within 30 days, the certificate will be revoked.

5. The Director notifies the certificate holder by certified mail, return receipt requested, of the decision to revoke the certificate.

6. Upon receiving the return receipt, the Director passes the information regarding the revocation to the maintainer of the Validated Products List so that summary information regarding the product can be removed from the list and certificate revoked status is indicated.

7. Records are generated documenting all activities connected with the revocation of the certificate, including correspondence with the product developer and removal of the product from the VPL.

[ISO65 4.2g, 4.6.2a, 12.2, CCMRA C.15, CCEVS Annex B]

7.3.6 Certificate Management Records

7.3.6.1 Issuing CC Certificate

- Copy of signed certificate
- Rationale for issuing certificate
- Summary of certificate information on VPL
- Notification to CCMRA partners of certificate issued

7.3.6.2 Recognition of CC Certificate Issued by CCMRA Partners

- Director CCEVS recommendation to signatories
- Signatory approval/disapproval
- Record of posting to VPL

7.3.6.3 Validated Products List

- Copy of certificate
- Identification of the VB that issued certificate
- Validation Report including security target
- Record of certificate revocation

7.3.6.4 Certificate Use Monitoring

- Document complaint (see section 4.6)
- VB action taken to investigate complaint
- VB recommended resolution and response
- Record of removal from VPL

7.3.6.5 Certificate Revocation

- Document evidence product no longer meets criteria for which it was evaluated or violation for conditions of use
- Letter to certificate holder and receipt for proposed certificate revocation

- Document evidence of corrective action
- Document final decision and return receipt
- Record of removal of product from VPL

8 Common Criteria Testing Laboratory Administration/Liaison

The Validation Body has responsibility for maintaining Approved Labs and Test Methods within the CCEVS. In performing this oversight, the Validation Body grants approval for a candidate CCTL to become an approved CCTL, modifies approval, coordinates with NVLAP to conduct audits, performs validator observations, and develops and maintains test methods and proficiency tests. The procedures for each of these are addressed below.

[ISO65 4.3]

8.1 Requirements for CCTL Approval

The Validation Body grants approval for candidate CCTLs to become a CCEVS CCTL. The conditions for approval are:

1. CCEVS-specific requirements

2. NVLAP accreditation

Rather than develop its own accreditation capabilities, the Validation Body has delegated the responsibility of CCTL accreditation to NVLAP. The Validation Body determines conformance to the additional CCEVS requirements.

When these two conditions for approval have been met, the candidate CCTL is approved by the Validation Body to conduct IT security evaluations for the specific test methods of its NVLAP accreditation and is registered on the NIAP Approved Laboratories List, and listed at the location(s) defined in Annex C.

[Scheme, Annex C]

8.1.1 CCEVS-Specific Requirements

The Validation Body imposes three CCEVS-specific requirements[2]:

a) A CCTL must reside within the U.S. and be a legal entity, duly organized and incorporated, validly existing, and in good standing under the laws of the state where the CCTL intends to do business; [3]

b) A CCTL must agree to accept U.S. Government technical oversight and validation of evaluation-related activities in accordance with the policies and procedures established by the CCEVS;

c) A CCTL must agree to accept U.S. Government participants in NIAP-selected CC evaluations conducted by the CCTL in accordance with the policies and procedures established by the CCEVS.

[2] The Validation Body reserves the right to levy additional CCEVS-specific requirements (either technical or administrative), as necessary, when deemed to be in the best interest of the U.S. Government and overall evaluation and validation effort.

[3] Assuming all other U.S. laws and regulatory requirements have been met, a foreign-owned enterprise could establish a testing laboratory in the U.S., become accredited under NVLAP, and be approved by NIAP as a CCTL. However, in order to meet the letter and spirit of the CCEVS requirements, a foreign-owned laboratory must maintain a substantial presence within the U.S., (i.e., a demonstrated, fully operational security testing capability) and all validation activities must be conducted from the U.S. facility.

The Validation Body will:

1. Verify the satisfaction of these requirements by inspecting the "Letter of Intent" submitted by a candidate CCTL. See Scheme Publication #1, *Common Criteria Evaluation and Validation Scheme for Information Technology Security—Organization, Management, and Concept of Operations.,* Annex H for a sample letter of intent

2. Document the findings of their verification and place the findings in Validation Body document and records control for a period of five years

3. Notify the candidate CCTL of its findings

4. Document an agreement with the CCTL when NVLAP accreditation has been completed

[Scheme, Annex C and H]

8.1.2 NVLAP Accreditation

NVLAP accreditation requires a candidate CCTL to demonstrate compliance with general technical and methodological criteria to conduct security evaluations of IT products. NVLAP will follow all instructions and requirements in the following documents to accredit a candidate CCTL:

1. NIST Handbook 150[4], *Procedures and General Requirements*

2. NIST Handbook 150-20, *Information Technology Security Testing—Common Criteria*

[Scheme, Section 3.3]

NVLAP issues two documents to candidate CCTLs that have been granted NVLAP accreditation: a Certificate of Accreditation and a Scope of Accreditation. Samples of accreditation documents for NVLAP and the steps to becoming accredited are described in Handbook 150-20, Sec. 285.23.

8.2 Establishing and Maintaining Test Methods

In the CCEVS, a test method is considered to be the set of procedures used by CCTLs to evaluate products and PPs. Each Common Criteria Evaluation Assurance Level (EAL) and the associated evaluation methodology for that EAL from the CEM, is a test method. A test method for PP evaluations and security targets also exists in the CC and CEM.

The CCEVS provides an *Approved Test Methods List* that identifies the CCEVS approved test methods that may be used by CCTLs. The *Approved Test Methods List* currently contains test methods for EAL1-4 and PP/ST evaluations. Additional test methods may be defined based on consumer requirements, technical viability, and CCEVS experience.

8.2.1 Test Method Development

The responsibilities of the Validation Body for developing new test methods are:

1. Develop test method requirements

[4] NIST Handbook 150 contains the requirements of ISO/IEC Guide 25, *General Requirements for the Competence of Calibration and Testing Laboratories*. ISO/IEC Technical Report 13233, *Information Technology-Interpretation of Accreditation Requirements in Guide 25 Accreditation of Information Technology and Telecommunications Testing Laboratories for Software and Protocol Testing Services* is used by NVLAP to interpret the requirements of ISO/IEC Guide 25 for CCTLs.

2. Obtain the necessary resources for test method development

3. Review and provide comments on draft test methods

4. Prototype the test method with groups representative of the target community

5. Approve all test methods

6. Place approved test methods on the CCEVS *Approved Test Methods List*

7. Submit the approved test method to NVLAP for use in accrediting labs

8.2.2 Test Method Maintenance

The Validation Body is jointly responsible for maintaining existing test methods along with other CCMRA participants. To accomplish this, the Validation Body will:

1. Work with the CCTLs to determine effectiveness and weaknesses in a test method

2. Perform yearly independent reviews of existing test methods

3. Assign resources to address test method changes

4. Coordinate findings with the other CCMRA participants

5. Update *Approved Test Methods List*

8.3 Extending or Reducing CCTL Scope of Accreditation

A NVLAP scope of accreditation is defined to be the specific *test methods* the CCTL has been accredited to use in conducting IT security evaluations. A candidate CCTL will choose the test methods it wishes to become accredited for from the CCEVS Approved Test Methods List developed by the Validation Body and which can be found at the location(s) defined in Annex C.

CCTLs wishing to expand or reduce their scope of accreditation, (i.e., adding or subtracting test methods) must apply to NVLAP for this change in scope of accreditation.

[Scheme, Annex C]

8.4 Renewal of Approval/Accreditation

To maintain its status as an NIAP-approved testing laboratory, a CCTL must ensure that its CCEVS approval and NVLAP accreditation remains current. CCTLs must have their CCEVS approved status reconfirmed yearly and their NVLAP accreditation status reconfirmed in accordance with NVLAP procedures. NVLAP procedures typically require reconfirmation to be done yearly, with an on-site assessment occurring every two years. Failure to retain CCEVS approval or NVLAP accreditation will result in withdrawal of the CCTL from the NIAP Approved Laboratories List. As noted in Section 8.3, these procedures will also be followed for a CCTL that has requested either an extension or reduction of accreditation.

The Validation Body will provide the CCTL a written description of the conditions and steps for renewal. This notification will be delivered 60 days before the renewal date.

If a CCTL satisfies the conditions for re-approval/re-accreditation (or extension/reduction of accreditation) the Validation Body will submit a written request to update the NIAP Approved Laboratories List.

If a CCTL fails to respond to the notification or has responded to the notification and fails re-approval/re-accreditation (or extension/reduction of accreditation), the provisions for withdrawal or suspension of approval/accreditation are applied as described in Section 8.5.

[Scheme, Annex C]

8.5 Withdrawal or Suspension of Approval/Accreditation

When the Validation Body determines that a CCTL has not complied with all CCEVS and NVLAP requirements, the CCTL may have its status withdrawn or suspended.

If a CCTL has its CCEVS approval or NVLAP accreditation *withdrawn* the CCTL must cease all CCEVS evaluation activities, is removed from the NIAP Approved Laboratories List, and must reapply for approval or accreditation as a CCTL.

If a CCTL has its CCEVS approval or NVLAP accreditation *suspended* the CCTL must *temporarily* cease all CCEVS evaluation activities until it resolves the condition(s) that caused the suspension. If the CCTL does not resolve the condition(s) that caused its suspension its CCTL status will be withdrawn.

The conditions for withdrawal and suspension of *CCEVS approval* are described in Scheme Publication #1, *Common Criteria Evaluation and Validation Scheme for Information Technology Security—Organization, Management, and Concept of Operations,* Annex C.

The conditions for withdrawal and suspension of *NVLAP accreditation* are described in NIST Handbooks 150 and 150-20.

When the Validation Body determines that a CCTL should have its CCTL status withdrawn or suspended it will notify a CCTL in writing 30 days before withdrawal or suspension date. The notification from the Validation Body will provide the CCTL with a description of the reason(s) for withdrawal or suspension and steps to follow to regain its status as a CCTL. If a CCTL fails to respond to the notification or comply with the notification, the Validation Body will:

1. Provide written notification to the CCTL that they are no longer an approved CCTL

2. Provide written notification to all sponsors of evaluations the CCTL is currently performing, that the CCTL is no longer an approved CCTL

3. Withdraw all resources from evaluations associated with the CCTL and remove from the *NIAP Approved Laboratories List*

[Scheme, Annex C]

8.6 Audits

CCTLs may be audited by NVLAP or the Validation Body to ensure that the CCEVS requirements continue to be met. The Validation Body will follow its internal auditing procedures during a CCTL audit (see Section 5.4). NVLAP will follow NIST Handbook 150 for its audit procedures. Auditing

by either NVLAP or the Validation Body will be coordinated between them such that conflicts and duplication do not occur.

CCTLs are required to define and maintain procedures for internal audits, and provide the results of the internal audits to the Validation Body and NVLAP. CCTLs are also required to inform the Validation Body of any changes in its status that may cause it to violate a CCEVS requirement, e.g., change in ownership, or NVLAP accreditation requirement.

[Scheme, Annex C]

8.7 Development and Maintenance of Proficiency Tests

NVLAP has determined that one element of accrediting CCTLs is to require a CCTL be tested. The purpose of these tests is to determine a candidate CCTL's potential to carry out the test methods for which they are seeking accreditation. These tests are referred to as proficiency tests (PT).

The Validation Body is responsible for the development and maintenance of PTs used during NVLAP accreditation. The Validation Body will work with NVLAP to ensure that PTs meet both CCEVS approval and NVLAP accreditation requirements.

8.7.1 PT Development

The responsibilities of the Validation Body for developing PTs are:

1. Develop Proficiency Test requirements

2. Obtain the necessary resources for Proficiency Test development

3. Review and provide comments on Proficiency Test objectives and draft Proficiency Tests

4. Prototype the Proficiency Test with groups representative of the target community

5. Approve all Proficiency Tests

8.7.2 PT Maintenance

The Validation Body is responsible for maintaining existing Proficiency Tests. To accomplish this, the Validation Body will:

1. Place all Proficiency Tests under configuration control.

2. Monitor changes in test methods for current NVLAP scopes of accreditation. This includes modification of existing test methods or the addition of new test methods

3. Review the results of CCTL tests to determine weaknesses in a Proficiency Test

4. Perform observations of CCTLs during evaluations, e.g. using a Validator, to determine weaknesses in a Proficiency Test

5. Perform yearly reviews of existing Proficiency Tests

6. Update Proficiency Tests based on the results of steps 1-4 above

All Proficiency Test updates are reviewed and approved by the Validation Body Director (or designee).

8.8 CCTL Administration Records

This section lists the records required to support the traceability and integrity of the CCTL Administration procedures.

8.8.1 Requirements for CCTL Approval Records

- Letter of intent from candidate CCTL to become a CCTL
- Candidate CCTL folder
- Response to candidate CCTL based on review of letter of intent
- Letter to NVLAP about the candidate CCTL
- NVLAP items as mandated by Handbooks 150 and 150-20
- Test results from NVLAP accreditation
- Notification letter to candidate CCTL approving or disapproving request to become a CCEVS CCTL

8.8.2 Establishing and Maintaining Test Methods Records

- Test method requirements
- Test method description (the actual test method)
- Approved test method list
- Test method prototype results
- Test method audits and reviews

8.8.3 Extending or Reducing CCTL Scope of Accreditation Records

- Form to request change in CCTL status (which should cause a change in the Approved Laboratories List, a notice to CCMRA participants, and notice to any sponsors or vendors that would be impacted)

8.8.4 Renewal of Accreditation/Approval Records

- Letter to CCTL informing them of conditions for renewal
- Letter (or other communication) from CCTL stating intent for renewal
- Letter to CCTL approving or disapproving renewal
- Form to request change in CCTL status (which should cause a change in the Approved Laboratories List, a notice to CCMRA participants, and notice to any sponsors or vendors that would be impacted)

8.8.5 Withdrawal of Suspension of Accreditation/Approval Records

- Letter to CCTL informing them of intent to withdraw or suspend the CCTL
- Response letter from CCTL related to VB intent letter
- Letter from CCTL informing VB of intent to withdraw
- Response letter from VB related to CCTL intent letter
- Form to request change in CCTL status (which should cause a change in the Approved Laboratories List, a notice to CCMRA participants, and notice to any sponsors or vendors that would be impacted)

8.8.6 Audit Records

- CCTL audit reports from CCEVS audit
- CCTL audit reports from CCTL audit
- Notice of change in CCTL status

8.8.7 Development and Maintenance of Proficiency Test Records

- Proficiency Test requirements
- Proficiency Test description (the actual PT)
- Proficiency Test prototype results
- Proficiency Test audits and reviews

9 Certificate Maintenance Program

A certificate is valid only for a specific version of a product or PP. Since most products that are evaluated continue to change as the products evolve and are enhanced with new features and capabilities, the Certificate Maintenance Program (CMP), implemented by the Validation Body, provides a means of establishing confidence that the assurance of the product is maintained without always requiring a formal re-evaluation. To participate in the CMP, the certificate applicant must state its intentions to participate during the initial product evaluation. There are three phases associated with the CMP, CMP Acceptance, CMP Monitoring, and Target of Evaluation Re-evaluation. These are described below. Detailed procedures for performing certificate maintenance are described in Scheme Publication #6, *Common Criteria Evaluation and Validation Scheme – Certificate Maintenance Program*.

9.1 CMP Acceptance, Monitoring and Product Re-evaluation

9.1.1 CMP Acceptance

1. The sponsor of an evaluation requests entrance into the CMP at the start of an evaluation by submitting assurance maintenance requirements along with product evaluation information.

2. The assurance maintenance requirements are evaluated by the CCTL along with other EAL requirements, and the evaluation is validated by the Validation Body.

3. The product is officially accepted into the CMP upon issuance of the initial Common Criteria Certificate.

9.1.2 CMP Monitoring

1. The sponsor of the evaluation submits proposed product changes to the Validation Body

2. Validation Body verifies that the changes are within scope and gives written approval to proceed

3. The sponsor selects a CCTL to conduct CMP related activities and delivers assurance maintenance documentation of the CCTL for evaluation

4. The CCTL reports the evaluation maintenance results to the Validation Body in a Certificate Maintenance Report (CMR)

5. The Validation Body issues a new certificate using procedures described in Section 8.1.

9.1.3 Product Re-evaluation

Re-evaluation may be scheduled as part of the Assurance Maintenance Plan in response to unforeseen significant changes to the product or its environment for which assurance maintenance activities were considered inappropriate. Reference Scheme Publication #6, *Common Criteria Evaluation and Validation Scheme – Certificate Maintenance Program* for a description of the detailed procedures for TOE Re-evaluation.

[ISO65 4.6, 4.6.2a,b,c, 12.2, 12.4, 13.2, 13.4, CCEVS, Annex F]

9.2 Certificate Maintenance Records

To assure the traceability and integrity of the certificate management function, the following events will be documented and stored as official Validation Body records:

- Certificate delivered to applicant (date sent and date confirmation received)
- Notice to applicant of reasons for not issuing a certificate based on an evaluation (letter or minutes of meeting discussing the matter)
- Certificate and Validation Report posted on the VPL (who posted information and date)
- Certificate and Validation Report removed from the VPL (who removed information and date)
- Applicant intent to participate in the CMP (applicant and date of intent)
- Notifications by supplier of changes in status of product (letter from supplier and date received by Validation Body)
- Validation Body surveillance activities and findings (date, who performed surveillance, type of surveillance, findings)
- Validation Body activities leading to withdrawal of a certificate (warnings to sponsor, correspondences with sponsor including time, date and persons involved in meetings or correspondences)
- Certificate withdrawal notification (formal notification letter and date)

Annex A. Glossary of Terms

This glossary contains definitions of terms used in the Common Criteria Scheme. These definitions are consistent with the definitions of terms in ISO Guide 2 and also broadly consistent with the Common Criteria and Common Methodology. However, the definitions of terms may have been amplified to add greater clarity or to interpret in the context of the evaluations conducted within the scheme.

Accredited: Formally confirmed by an accreditation body as meeting a predetermined standard of impartiality and general technical, methodological, and procedural competence.

Accreditation Body: An independent organization responsible for assessing the performance of other organizations against a recognized standard, and for formally confirming the status of those that meet the standard.

Agreement on the Mutual Recognition of Common Criteria Certificates in the field of IT Security: An agreement in which the Parties (i.e., signatories from participating nations) agree to commit themselves, with respect to IT products and protection profiles, to recognize the Common Criteria certificates which have been issued by any one of them in accordance with the terms of the agreement.

Appeal: The process of taking a complaint to a higher level for resolution.

Approval Policy: A part of the essential documentation of the Common Criteria Evaluation and Validation Scheme, setting out the procedures for making an application to be approved as a CCTL and placed on the NIAP Approved Laboratories List and for the processing of such applications and of the requirements which an applicant must fulfill in order to qualify.

Approved: Assessed by the NIAP Validation Body as technically competent in the specific field of IT security evaluation and formally authorized to carry out evaluations within the context of the Common Criteria Evaluation and Validation Scheme.

Approved Laboratories List: The list of approved CCTLs authorized by the NIAP Validation Body to conduct IT security evaluations within the Common Criteria Evaluation and Validation Scheme.

Approved Test Methods List: The list of approved test methods maintained by the NIAP Validation Body which can be selected by a CCTL in choosing its scope of accreditation, that is, the types of IT security evaluations that it will be authorized to conduct using NIAP-approved test methods.

Assurance Maintenance Plan: Part of the formal assurance maintenance documentation submitted to the Validation Body by the sponsor of an evaluation (as part of the initial TOE evaluation) that identifies the plans and procedures a developer is to implement in order to ensure that the assurance that was established in the validated TOE is maintained as changes are made to the TOE or its environment.

Availability: The prevention of unauthorized withholding of information resources.

Certificate Maintenance Program: A program within the Common Criteria Scheme that allows a sponsor to maintain a Common Criteria certificate by providing a means (through specific assurance maintenance requirements) to ensure that a validated TOE will continue to meet its security target as changes are made to the IT product or its environment.

Certificate Maintenance Report: A report prepared by a CCTL for the Validation Body detailing the results of their evaluation maintenance activities conducted on behalf of a sponsor.

Certificate Maintenance Summary Report: An annual report prepared by a sponsor for the Validation Body providing a summary of all certificate maintenance activities conducted during the previous year.

Common Criteria (CC): Common Criteria for Information Technology Security Evaluation, the title of a set of documents describing a particular set of IT security evaluation criteria.

Common Methodology (CEM): Common Methodology for Information Technology Security Evaluation, the title of a technical document which describes a particular set of IT security evaluation methods.

Common Criteria Certificate: A brief public document issued by the NIAP Validation Body under the authority of NIST and NSA which confirms that and IT product or protection profile has successfully completed evaluation by a CCTL. A Common Criteria certificate always has associated with it, a validation report.

Common Criteria Evaluation and Validation Scheme (CCEVS): The program developed by NIST and NSA as part of the National Information Assurance Partnership (NIAP) establishing an organizational and technical framework to evaluate the trustworthiness of IT products and protection profiles.

Common Criteria Testing Laboratory (CCTL): Within the context of the Common Criteria Evaluation and Validation Scheme, an IT security evaluation facility, accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the NIAP Validation Body to conduct Common Criteria-based evaluations.

Complaint: A written formal allegation or disagreement against a party.

Complainant: The party who makes the complaint.

Confidentiality: The prevention of unauthorized disclosure of information.

Deliverables List: A document produced by a CCTL containing the definition of the documents comprising the security target, all representations of the TOE, and developer support required to conduct an IT security evaluation in accordance with the laboratory's evaluation work plan.

Evaluation: The assessment of an IT product against the Common Criteria using the Common Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria suing the Common Methodology to determine if the profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.

Evaluation and Validation Scheme: The systematic organization of the functions of evaluation and validation within a given country under the authority of a Validation Body in order to ensure that high standards of competence and impartiality are maintained and that consistency is achieved.

Evaluation Schedule: The schedule established by a CCTL for the conduct of an IT security evaluation.

Evaluation Technical Report: A report giving the details of the findings of an evaluation, submitted by the CCTL to the NIAP Validation Body as the principal basis for the validation report.

Evaluation Work Plan: A document produced by a CCTL detailing the organization, schedule, and planned activities for an IT security evaluation.

Integrity: The prevention of the unauthorized modification of information.

Interpretation: Expert technical judgement, when required, regarding the meaning or method of application of any technical aspect of the Common Criteria and/or Common Methodology.

IT Product: A package of IT hardware, software, and/or firmware providing functionality designed for use or incorporation within a multiplicity of IT systems.

IT System: A group of IT products, either tightly or loosely coupled, working together in a specific configuration to provide a capability or system solution to a consumer in response to a stated need.

IT Security Evaluation Criteria: A compilation of the information which needs to be provided and actions which need to be taken in order to provide grounds for confidence that security evaluations will be carried out effectively and to a consistent standard.

IT Security Evaluation Methodology: A methodology which needs to be used by evaluation facilities in applying IT security evaluation criteria in order to give grounds for confidence that evaluations will be carried out effectively and to a consistent standard.

National Voluntary Laboratory Accreditation Program (NVLAP): The U.S. accreditation authority for CCTLs operating within the NIAP Common Criteria Evaluation and Validation Scheme.

NIAP Validation Body: A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the Common Criteria Evaluation and Validation Scheme.

Observation Reports: A report issued to the NIAP Validation Body by a CCTL or sponsor identifying specific problems or issues related to the conduct of an IT security evaluation.

Party: A signatory to the *Agreement on the Mutual Recognition of Common Criteria Certificates in the field of IT Security.*

Protection Profile: An implementation independent set of security requirements for a category of IT products which meet specific consumer needs.

Recognition of Common Criteria Certificates: With respect to the Agreement on the Mutual Recognition of Common Criteria Certificates in the Field of IT Security, acknowledgment by one Party of the validity of the Common Criteria certificates issued by another Party.

Scope of Accreditation: The NIAP-approved test methods for which a CCTL has been accredited by NVLAP.

Security Target: A specification of the security required (both functionality and assurance) in a Target of Evaluation (TOE), used as a baseline for evaluation under the Common Criteria. The security target specifies the security objectives, the threats to those objectives, and any specific security mechanisms that will be employed.

Shadow Evaluations: The placement of technical personnel in selected CCTLs by the NIAP Validation Body for the express purpose of observing and/or participating in Common Criteria-based evaluations in a variety of information technology areas.

Sponsor: The person or organization that requests a security evaluation of an IT product or protection profile.

Target of Evaluation (TOE): An IT product or group of IT products configured as an IT system and associated documentation that is the subject of a security evaluation under the Common Criteria. Also, a protection profile that is the subject of a security evaluation under the Common Criteria.

Test Method: An evaluation assurance package from the Common Criteria and the associated evaluation methodology for that assurance package from the Common Methodology.

Validation: The process carried out by the NIAP Validation Body leading to the issue of a Common Criteria certificate.

Validated Products List: A publicly available document issued periodically by the NIAP Validation Body giving brief particulars of every IT product or protection profile which holds a currently valid Common Criteria certificate awarded by that body and every product or profile validated or certified under the authority of another Party for which the certificate has been recognized.

Validation Report: A publicly available document issued by he NIAP Validation Body which summarizes the results of an evaluation and confirms the overall results, (i.e., that the evaluation has been properly carried out, that the Common Criteria, the Common Methodology, and the scheme-specific procedures have been corectly applied and that the conclusions of the evaluation technical report are consistent with the evidence adduced).

Annex B. Scheme Publications

The following is a list of CCEVS Publications

Scheme Publication #1 *NIAP Common Criteria Evaluation and Validation Scheme for IT Security Organization, Management, and Concept of Operations*

Scheme Publication #2 *NIAP Common Criteria Evaluation and Validation Scheme for IT Security Validation Body Standard Operating Procedures*

Scheme Publication #3 *NIAP Common Criteria Evaluation and Validation Scheme for IT Security Technical Oversight and Validation Procedures*

Scheme Publication #4 *NIAP Common Criteria Evaluation and Validation Scheme for IT Security Guidance to Common Criteria Testing Laboratories*

Scheme Publication #5 *NIAP Common Criteria Evaluation and Validation Scheme for IT Security Guidance to Sponsors of IT Security Evaluations*

Scheme Publication #6 *NIAP Common Criteria Evaluation and Validation Scheme for IT Security Certificate Maintenance Program*

NIST Handbook 150 *Procedures and General Requirements*

NIST Handbook 150-20 *Information Technology Security Testing—Common Criteria*

Validated Products List - includes a list of validated IT products and PPs that have received Common Criteria certificates

Validation Reports - for products that have received a CC certificate

NIAP Approved CCEVS Laboratories List

Validation Body Annual Report

CCEVS Newsletters

Official Notices/addendums

General information about the CCEVS program

- Information and application for becoming a CCTL
- Information and application for entering the CCEVS

Annex C. CCEVS Contact Information

Public information about the CCEVS may be retrieved from the NIAP Web site at **http://niap.nist.gov** or can be requested by phone or mail. Phone inquiries may be made to 301-975-3247. Mail inquiries may be directed to:

Director
Common Criteria Evaluation & Validation Scheme
National Information Assurance Partnership
National Institute of Standards & Technology
100 Bureau Drive, Mail Stop 8930
Gaithersburg, MD 20899-8930

Annex D. Validation Body Staff

This Annex includes the names, titles and phone numbers of key Validation Body personnel. A resume is on file with the CCEVS Data/Records Manager and is available in hardcopy upon request.

Director: Thomas Anderson
Mailing address: National Security Agency
9800 Savage Road, Suite 6740
Ft. George G. Meade, MD 20755-6740
E-Mail: teander@missi.ncsc.mil

Deputy Director: Arnold Johnson
Mailing address: National Institute of Standards and Technology
100 Bureau Drive, Mail Stop 8930
Gaithersburg, MD 20899-8930
E-Mail: arnold.johnson@nist.gov

Quality Manager: Arnold Johnson
Mailing address: National Institute of Standards and Technology
100 Bureau Drive, Mail Stop 8930
Gaithersburg, MD 20899-8930
E-Mail: arnold.johnson@nist.gov

Technical Oversight Manager:
Mailing address:
E-Mail:

CCTL Administration/Liaison: Patricia Toth
Mailing address: National Institute of Standards and Technology
100 Bureau Drive, Mail Stop 8930
Gaithersburg, MD 20899-8930
E-Mail: patricia.toth@nist.gov

Certificate Maintenance Manager:
Mailing address:
E-Mail:

Resource Manager: Janine Pedersen
Mailing address: National Security Agency
9800 Savage Road, Suite 6740
Ft. George G. Meade, MD 20755-6740
E-Mail: jspeder@missi.ncsc.mil

Data/Records Manager: Rebecca Galanakis
Mailing Address: National Security Agency
9800 Savage Road, Suite 6740
Ft. George G. Meade, MD 20755-6740
E-Mail: rmgalan@missi.ncsc.mil

Annex E. Approved Contractor List

This Annex includes the list of contractors that have been approved to perform duties for the Validation Body:

Aerospace Corporation

Institute for Defense Analysis

Mitre Corporation

Mitretek Systems

Annex F. Sample Non-Disclosure Agreement

Statement of Personal Responsibility
For Non-Disclosure of Proprietary Information

As an employee of the National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS), you may become aware of certain information which is proprietary to a specific vendor and/or Common Criteria Testing Laboratory (CCTL). This proprietary information is provided to the NIAP CCEVS with the assurance that said proprietary information will not be disclosed to personnel not authorized to see it.

This notice serves to remind you of the penalty for disclosure of proprietary information as described in 18 USC 1905 (Disclosure of Confidential Information, Generally) reproduced below. Note that all proprietary information must be so identified by the vendor and/or CCTL providing such information.

1905. Disclosure of Confidential Information Generally

Whoever, being an officer or employee of the United States or of any department or agency thereof, any person acting on behalf of the Office of Federal Housing Enterprise Oversight, or agent of the Department of Justice as defined in the Antitrust Civil Process Act (15 U.S.C. 1311-1314), publishes, divulges, discloses, or makes known in any manner or to any extent not authorized by law any information coming to him in the course of his employment or official duties or by reason of examination or investigation made by, or return, report or record made to or filed with, such department or agency or officer or employee thereof, which information concerns or relates to the trade secrets, processes, operations, style of work, or apparatus, or the identity, confidential statistical data, amount or source of any income, profits, losses or expenditures of any person, firm, partnership, corporation, or association, or permits any income return or copy thereof or any book containing any abstract or particulars thereof to be seen or examined by any person except as provided by law, shall be fined not more than $1,000, or imprisoned not more than one year, or both, and shall be removed from office or employment.

(As amended Oct. 28, 1992, Pub L 102-550, Title XIII, 1353, 106 Stat.3970)

I acknowledge that I have read and I understand the Statement of Personal Responsibility.

_____ _____

Printed Name Signature & Date